UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/675,262	09/28/2000	Jesse R. Walker	42390P9007	3019

8791 7590 11/02/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CHO, UN C	

ART UNIT	PAPER NUMBER
2687	

DATE MAILED: 11/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/675,262	WALKER, JESSE R.	
	Examiner	Art Unit	
	Un C. Cho	2687	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 August 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 8/15/2005 has been entered.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1, 2, 4, 15, 16, 22, 23 and 27 are rejected under 35 U.S.C. 102(e) as being anticipated by Nessett et al. (US 6,920,559 B1).

Regarding claim 1, Nessett discloses a method for establishing secured roaming among a wireless station, a first and a second access points (Nessett, Col. 7, lines 8 – 11), comprising: the first access point (AP1, Fig. 2, 210) request a first ticket from an authentication server (RADIUS server – authentication

server; Fig. 2, 250) and using the first ticket to establish a first secured session between the first access point and the wireless station (WC, Fig. 2, 220) (in order for WC to authenticate, AP1 sends a request to the authentication server Fig. 2, 250 and authentication resource is transmitted back to AP1 so that it can establish a primary secured session with WC, Nessett, Col. 9, lines 21 – 35); and in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station (since Nessett already takes into consideration that WC moves from one physical location (AP1) to a second physical location (AP2) after successfully completing the primary authentication protocol among WC, AP1 and the authentication server, the authentication server transmits a key lease (resulting second ticket) to the WC; Nessett, Col. 6, line 57 through Col. 7, line 11), the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point (the key lease is used to establish a secured session between the WC and the second AP, Nessett, Col. 7, lines 12 – 28).

Regarding claim 2, Nessett discloses applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong

to the same group, and wherein the wireless station can only access another access point within the same group identified by the group identity using the second ticket (Nessett, Col. 7, line 56 through Col. 8, line 4).

Regarding claim 4, Nessett discloses that a first and a second session keys have limited lifetime (a key lease comprise a key lease period for indicating a length of time in which they key lease is valid, Nessett, Col. 7, lines 34 – 45)

Regarding claim 15, Nessett discloses a secured wireless roaming system, comprising: a wired medium; a wireless medium (wireless connection, Fig. 2, 230); an authentication server coupled to the wired medium (RADIUS or authentication server, Fig. 2, 250); a wireless station coupled to the wireless medium (WC, Fig. 2, 220); and an access point coupled to the wireless medium and the wired medium (AP1 – APX coupled to the wired medium Fig. 2, 240, 241 and wireless medium, Fig. 2, 230), wherein the access point comprises a first control unit, comprising the first access point (AP1, Fig. 2, 210) requesting a first ticket from an authentication server (RADIUS server – authentication server; Fig. 2, 250) and using the first ticket to establish a first secured session between the first access point and the wireless station (WC, Fig. 2, 220) (in order for WC to authenticate, AP1 sends a request to the authentication server Fig. 2, 250 and authentication resource is transmitted back to AP1 so that it can establish a primary secured session with WC, Nessett, Col. 9, lines 21 – 35); and in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to

the authentication server and relaying a resulting second ticket from the authentication server to the wireless station (since Nessett already takes into consideration that WC moves from one physical location (AP1) to a second physical location (AP2) after successfully completing the primary authentication protocol among WC, AP1 and the authentication server, the authentication server transmits a key lease (resulting second ticket) to the WC; Nessett, Col. 6, line 57 through Col. 7, line 11), the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point (the key lease is used to establish a secured session between the WC and the second AP, Nessett, Col. 7, lines 12 – 28).

Regarding claim 16, the claim is interpreted and rejected for the same reason as set forth in claim 2.

Regarding claim 22, Nessett discloses that wherein the second ticket is only valid for the second secured session between the wireless station and the second access point (the key lease is used to establish a secured session between the WC and the second AP, Nessett, Col. 7, lines 12 – 28).

Regarding claim 23, Nessett discloses wherein the second ticket is only valid for the second secured session for a predetermined period of time (a key lease comprise a key lease period for indicating a length of time in which they key lease is valid, Nessett, Col. 7, lines 34 – 45).

Regarding claim 27, the claim is interpreted and rejected for the same reason as set forth in claim 1.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 3, 5 – 14, 17 – 21 and 24 – 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in view of Brown et al. (US 5,689,563 B1).

Regarding claim 3, Nessett as applied above discloses that the authentication server dynamically generating a first and a second session keys to include in the first and the second tickets (Nessett, Col. 9, lines 30 – 35).

However, Nessett as applied above does not specifically disclose that the authentication server encrypts the first and the second tickets with a first and a second encryption keys. In analogous art, Brown discloses that the authenticating unit generates a first and a second session keys to include in the first and the second tickets and the authenticating unit encrypting the first and the second tickets with a first and a second encryption keys (Brown, Col. 3, line 63 through Col. 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the art the time the invention was made to provide the technique of Brown

to the system of to create an encryption technique to alleviate problems associated with packetized data to be more efficient and secure.

Regarding claim 5, Nessett in view of Brown as applied above discloses the first fixed network communication unit 130 appending application specific information to the second ticket to formulate a combined message and the first fixed network communication unit encrypting the combined message with the first session key (Brown, Col. 6, lines 35 – 54).

Regarding claim 6, Nessett in view of Brown as applied above discloses the application specific information further comprises the first fixed network communication unit 130 selected instant specific information and random challenge (RAND) (Brown, Col. 6, lines 14 – 21 and Col. 7, lines 39 – 48).

Regarding claim 7, Nessett in view of Brown as applied above discloses an access point (Fixed network communication unit, Brown, Fig. 1, 130) in a secured wireless roaming system, comprising an antenna (an antenna, Brown, Fig. 1, 154); a filter coupled to the antenna (a filter is inherently coupled to the antenna), a receiver and a transmitter coupled to the filter (a receiver and a transmitter, Brown, Fig. 1, 152, coupled to the filter) and a control unit coupled to the receiver and the transmitter and coupled to a wired-network connection interface (microprocessor, Brown, Fig. 1, 148, coupled to the receiver and the transmitter, which forms a switch center, Brown, Fig. 1, 128, and the switch center is coupled to a wired-network such as PSTN, Brown, Fig. 1, 132), wherein the control unit further comprises an authentication protocol engine (switch

center comprises a database, Brown, Fig. 1, 136; Brown, Col. 5, lines 54 – 66) that the first access point (AP1, Fig. 2, 210) request a first ticket from an authentication server (RADIUS server – authentication server; Fig. 2, 250) and using the first ticket to establish a first secured session between the first access point and the wireless station (WC, Fig. 2, 220) (in order for WC to authenticate, AP1 sends a request to the authentication server Fig. 2, 250 and authentication resource is transmitted back to AP1 so that it can establish a primary secured session with WC, Nessett, Col. 9, lines 21 – 35); and in response to a second ticket request from the wireless station through the first secured session, the first access point forwarding the second ticket request to the authentication server and relaying a resulting second ticket from the authentication server to the wireless station (since Nessett already takes into consideration that WC moves from one physical location (AP1) to a second physical location (AP2) after successfully completing the primary authentication protocol among WC, AP1 and the authentication server, the authentication server transmits a key lease (resulting second ticket) to the WC; Nessett, Col. 6, line 57 through Col. 7, line 11), the second ticket being different than the first ticket, wherein the second ticket is used to establish a second secured session between the wireless station and the second access point (the key lease is used to establish a secured session between the WC and the second AP, Nessett, Col. 7, lines 12 – 28).

Regarding claim 8, Nessett in view of Brown as applied above discloses that a switch center (Fig. 1, 128) within the fixed network communication unit decrypting the second ticket request (Brown, Col. 8, lines 16 – 24).

Regarding claim 9, the claim is interpreted and rejected for the same reason as set forth in claim 3.

Regarding claim 10, Nessett in view of Brown as applied above discloses that the first and the second session keys have limited lifetime (a key lease comprise a key lease period for indicating a length of time in which they key lease is valid, Nessett, Col. 7, lines 34 – 45).

Regarding claim 11, the claim is interpreted and rejected for the same reason as set forth in claim 5.

Regarding claim 12, the claim is interpreted and rejected for the same reason as set forth in claim 6.

Regarding claim 13, the claim is interpreted and rejected for the same reason as set forth in claim 7.

Regarding claim 14, Nessett in view of Brown as applied above discloses applying the second ticket and a group identity shared by the first and the second access points to establish a second secured session between the wireless station and the second access point, the group identity identifying that the first and second access points belong to the same group, and wherein the wireless station can only access another access point within the same group identified by

the group identity using the second ticket (Nessett, Col. 7, line 56 through Col. 8, line 4).

Regarding claim 17, the claim is interpreted and rejected for the same reason as set forth in claim 8.

Regarding claim 18, the claim is interpreted and rejected for the same reason as set forth in claim 3.

Regarding claim 19, the claim is interpreted and rejected for the same reason as set forth in claim 10.

Regarding claim 20, the claim is interpreted and rejected for the same reason as set forth in claim 5.

Regarding claim 21, the claim is interpreted and rejected for the same reason as set forth in claim 6.

Regarding claim 24, Nessett in view of Brown as applied above discloses the wireless station providing an identification of the wireless station to the first access point (WC provides a first identifier to the first AP, Nessett, Col. 7, lines 17 – 23); the first access point obtaining the first ticket from the authentication server; and the first access point establishing the first secured session using the newly obtained first ticket (in order for WC to authenticate, AP1 sends a request to the authentication server Fig. 2, 250 and authentication resource is transmitted back to AP1 so that it can establish a primary secured session with WC, Nessett, Col. 9, lines 21 – 35).

Regarding claim 25, the claim is interpreted and rejected for the same reason as set forth in claim 14.

Regarding claim 26, Nessett in view of Brown as applied above discloses wherein the second secured session is established based on the second session key and the group ID (Nessett, Col. 12, lines 40 – 46).

Response to Arguments

6. Applicant's arguments with respect to claims 1 – 27 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Nessett et al. (US 6,766,453 B1) discloses authenticated Diffie-Hellman key agreement protocol where the communicating parties share a secret key with a third party.

Kou (US 6,363,365 B1) discloses mechanism for secure tendering in an open electronic network.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Un C. Cho whose telephone number is (571) 272-7919. The examiner can normally be reached on M ~ F 8:00AM to 4:30PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lester Kincaid can be reached on (571) 272-7922. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Un C Cho
Examiner
Art Unit 2687

10/25/05

10/30/05
LESTER G. KINCAID
SUPERVISORY PRIMARY EXAMINER